BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation

Arab Journal of Basic and Applied Sciences

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tabs20

BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation

Hasan Al-Aswad, Wael M. El-Medany, Chitra Balakrishna, Nedal Ababneh & Kevin Curran

To cite this article: Hasan Al-Aswad, Wael M. El-Medany, Chitra Balakrishna, Nedal Ababneh & Kevin Curran (2021) BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation, Arab Journal of Basic and Applied Sciences, 28:1, 154-171, DOI: 10.1080/25765299.2020.1870812

To link to this article: https://doi.org/10.1080/25765299.2020.1870812

ARAB JOURNAL OF BASIC AND APPLIED SCIENCES
2021, VOL. 28, NO. 1, 154–171
https://doi.org/10.1080/25765299.2020.1870812

University of Bahrain
Taylor & Francis
Taylor & Francis Group

BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation

Hasan Al-Aswad[a], Wael M. El-Medany[a], Chitra Balakrishna[b], Nedal Ababneh[c] and Kevin Curran[d]

[a]Department of Computer Engineering, University of Bahrain, Sakhir, Bahrain; [b]Faculty of Science, Technology, Engineering & Mathematics, The Open University, Milton Keynes, UK; [c]Department of Information Security Engineering Technology, Abu Dhabi Polytechnic, Abu Dhabi, UAE; [d]Computing, Engineering & Intelligent Systems, Ulster University, Coleraine, UK

ABSTRACT

Smart cities achieved digital transformation of patients' health records through the use of new technology in IoT healthcare industry. Such technologies of using IoT and remote patient monitoring systems have become dramatically fundamental to reduce the movement of patients, and hence reducing the risk of spreading Covid-19 infection. The Ministry of Health in the Kingdom of Bahrain strives to achieve digital transformation in the healthcare industry, where the National Health Information System (I-SEHA) was launched to provide higher-quality health services. The system interconnects the public healthcare institutes, allowing access to patient's data from any location without the hassle of moving the files physically. Digitization of medical data of patients and sharing some of the data with other institutions outside the protected networks may lead to major privacy and integrity concerns. This paper introduces Blockchain-based Zero-Knowledge Proof (BZKP) model, which is an IoT-based patient-centric model that fuses a zero-knowledge proof solution to be developed for protecting patient's privacy, and ensures patients prior consent on any access to their data including their health status and account balance. The proposed model is developed to provide a robust and scalable architecture for data sharing, which protects the privacy of sensitive data while maintaining high availability. It also provides strong trust and integrity of data by using the immutability features of the blockchain. BZKP is based on pre-approved blockchain access tokens to address challenges of accountability and privacy in Bahrain smart cities. As a result, the model provides a secure and trusted access model between different stakeholders to share patient data while maintaining privacy, trust, and high availability. The zero-knowledge proof can be used with the smart contracts, which provides programmable actions that can be used for automating the prescriptions dispensation process for private pharmacies in a decentralized manner with high confidence. Finally, it recommends enhanced electronic key (eKey) procedures used by eGovernment of the Kingdom of Bahrain to update the smart card which stores the personal keys for protecting patient's privacy and provide better consent.

ARTICLE HISTORY
Received 3 August 2020
Revised 23 December 2020
Accepted 26 December 2020

KEYWORDS
Blockchain; COVID-19; cybersecurity; IoT healthcare; smart city; zero-knowledge proof

1. Introduction

Smart city brings together data, digital technologies, and infrastructure for improving life qualities of people and enhancing their interactions with their surrounding environment. Internet of things (IoT) improves the quality of services in smart cities by using different types of tiny and smart sensors that are used to collect data and then use insights gained from that data to manage assets, resources, and services efficiently. This has increased the importance of cybersecurity and trust in the different types of data being collected. The cybersecurity risks and opportunities will affect major sectors across the smart cities, including the financial services, healthcare, transportation, and power. There are many different techniques and algorithms for improving the security and privacy in IoT healthcare applications in smart cities (Al-Aswad, Hasan, Elmedany, Ali, & Balakrishna, 2019; Alharam & El-Madany, 2017b; Alromaihi et al., 2018; Djenna & Saïdouni, 2018; Unnikrishnan, 2019).

Blockchain technology designed to share trusted and verifiable data between various stakeholders continuously and securely. The technology can be integrated into various digital services, which makes it interesting to invest in for the development of digital services in many countries around the world. The blockchain is a digital ledger where data

CONTACT Wael M. El-Medany welmedany@uob.edu.bh Department of Computer Engineering, University of Bahrain, PO Box 32038, Sakhir, Bahrain.

transactions are visible to the participant or peers. A dynamic consent protocol allows users to grant, deny or revoke access to data for different reasons according to their preferences. Whenever you add a block, it is then connected to the previous one in a way, which cannot be altered. We can use the blockchain technology for securing smart card data, to prove the integrity of the data in a decentralized way. All of these features offered by blockchain participate in the improvement of smart city services and promote the development of smart cities. A comprehensive survey on the application of blockchain technology to smart cities has been conducted in Xie et al. (2019) focusing on smart healthcare, smart transportation systems, and smart grid. The study discussed the challenges and research issues. Blockchain technology offers a different approach to store information in the database by dealing with records as transactions. It uses a block to store each data in the database. Each block has cryptographic information combined between that data and a link from the previous block. A chain of blocks are maintained to establish trust, hence if the block within the chain is valid, the block, as well as the previous blocks linked to it, are also valid.

A blockchain provides a secure database which maintains a constantly expanding list of records. The chain structure gives the blockchain self-resistance to modification by outside sources. The blockchain technology concept was introduced in 2008 but it is still considered relatively new to provide a new trust model across different smart communities, IoT and even in constructing new business models. This technology has enabled a long list of possible applications in smart city context since the connected devices, the diversity and speed of data are much faster than normal, forming Big Data. Blockchain has been used in the healthcare sector to secure the transmission of Electronic Health Record (EHR) of patient between the different entities in healthcare industry (Dubovitskaya, Xu, Ryu, Schumacher, & Wang, 2017; Khatoon, 2020). The private healthcare centers or hospitals are allowed to add new information to the patient's medical record using the blockchain model. The results of the conduct review in Hasselgren, Kralevska, Gligoroski, Pedersen, and Faxvaag (2019) indicate that the electronic health record is the most targeted area in healthcare using blockchain technology. The study shows that the use of blockchain in healthcare industry is increasing exponentially. Another study carried out by authors in Khan, Asif, Ahmad, Alharbi, and Aljuaid (2020), this research focuses on the application of blockchain technology in healthcare. In this research, their contribution of four-layers custom blockchain models related to precision medicine and the clinical trial was notable. Moreover, a mobile application model was introduced for the automation of medical records without compromising privacy was also a prominent contribution.

In Dwivedi, Srivastava, Dhar, and Singh (2019), authors introduced a model that used blockchain for IoT based healthcare devices in smart cities application. This research provides a secure management system for healthcare that resolve many of the resource-constrained issues for IoT devices in smart cities. An Access Control Policy Algorithm using blockchain has been introduced in Tanwar, Parekh, and Evans (2020) that improves data accessibility among healthcare providers. The study used the concept of a chain code to improve sharing of electronic health records for patient and improving some of the limitations in the current healthcare system. With the emerging technologies of the digital era, the need for trusted data becomes very important. The smart city hub connects different systems such as solar energy, smart cars, and smart buildings. This data needs to be shared between these systems to make proper decisions. Of course, data integrity is of paramount importance here. The blockchain model solves the problem of sharing trusted data but it requires further layers to protect the privacy and to deploy access control. The constructed model can be a unified model for different communities and systems as there are many used cases which require a model for sharing trusted data. With the success of developing this model, researchers can use it to ensure its trustiness, accountability, and availability (Dubovitskaya et al., 2017; Khatoon, 2020).

Recently, cities around the world are moving beyond the pilot stage and using data and digital technologies to deliver results that are more relevant and meaningful to residents. Providing instant information about weather, traffic, health services, and safety alerts to the public. Twenty two countries in Europe have signed the establishment of a European Blockchain Partnership. The European Commission launched the European Union Blockchain Observatory and Forum in February 2018 and also invested more than EUR 80 million in projects supporting the use of blockchain in technical and societal areas (Dwivedi et al., 2019; Tanwar et al., 2020).

The Ministry of Health (MoH) is planning to introduce a national insurance system where any resident can access healthcare services in public or private sectors based on his/her insurance scheme. The various healthcare organizations will need to share the patient medical data. The data should be available to any authorized entity within the healthcare system while maintaining its privacy and integrity. According to official data published in 'Bahrain in

Table 1. Number of hospitals in the Kingdom of Bahrain (Alharam & El-Madany, 2017b).

	Year				
	2011	2012	2013	2015	2020
Government Hospitals	6	6	6	6	10
Maternity Hospitals	3	3	1	1	1
Health Centers	24	26	27	28	28
Private Hospitals and Health Units	15	15	16	18	18

Figures' by Bahrain government (Information & eGovernment A (iGA) of Bahrain, 2016), the number of patients who visited the government hospitals and public health units is 5,992,000 while in the private hospitals they were 1,394,000. From Table 1, it is evident that the number of private hospitals is three times more than the number of government hospitals. This increases the necessity of having a trusted model for sharing patient's data among these organizations. Refer to Table 1 for more details.

In the Middle East, Dubai is planning to host all its government operations on blockchain as part of the Smart Dubai 2021 initiative. MoH in Bahrain has developed a vision to provide digital transformation of services and operations, aiming to move towards smart city digital solution.

In this paper, a blockchain-based model has been introduced for sharing electronic health records of patients in Bahrain smart cities using IoT technology. The proposed model can provide trusted and unchangeable stored data across different parties in healthcare industry, and mitigating the risk of COVID-19 spreading. The paper conducted a literature review about blockchain technology and its benefits in different dimensions but primarily as an enabler in the smart city and to show how it can provide trusted and unchangeable stored data across different parties as well as to identify the strengths and weaknesses of different available healthcare data sharing models.

A risk assessment would be conducted on the current medical health record project I-SEHA and compared to the proposed BZKP model to reduce risks related to the availability of the system, and integrity of the data stored on it. The use of the blockchain is to ensure that the data is stored on the blockchain without affecting performance and capacity, while other data will be off-chain to provide high scalability and privacy (S. Council of Health, 2017).

In addition, to analyze the risk of the data being shared and how to mitigate any risks that occur. Then to construct a trusted model for sharing medical data between different organizations with proper authorization channels allowing them to add new reports and data where applicable without affecting the trust. The accountability of any changes with respect to the trust of data will be maintained via the blockchain-based system. To illustrate the process of purchasing medicine from participating parties by using smart contracts for checking the insurance credit and verifying medical prescriptions. To propose policies and procedures on sharing medical data related to which data can be shared and which organizations or entities are entitled to access this data i.e. pharmacies, individuals, and private health centers (Xia et al., 2017).

The remainder of this paper is organized as follows. Section 2 describes the related works on Blockchain, and its application on healthcare. Section 3 defines the blockchain and discusses its fundamentals and major technologies. Then, Sect. 4, discusses security of blockchain. Section 5, describes our proposed secure blockchain architecture, Sect. 6 discuss the achieved results, and finally, Sect. 7 concludes the paper.

2. Related work

Several blockchain-based models have been developed to enhance the security and protect the privacy of healthcare systems. The models vary in two aspects. First, how the data is stored, whether on the blockchain itself or off-blockchain, and this is important to protect the privacy of the information and scalability of the entire system. Second, what mining method is used and will it give a competent performance over other approaches. Healthcare is a regulated industry and its applications are required to be highly trustworthy to ensure the security and privacy of patients and to maintain the highest availability of the system.

2.1. Providing privacy in bloackchain

The aim of blockchain original model is to provide trust over data, where the data is then distributed over a decentralized model to extend the availability, however, this model incurs a privacy risk of sensitive data, there are several models that have been suggested to mitigate this problem. Smart buildings are connecting operational systems like lighting, air conditioning and other IoT devices including IP cameras and smart TVs. Automated processes are used to increase reliability and efficiency, however, there are risks involved in these processes (Xie et al., 2019). Cyberbit addresses some challenges including tampering with IP camera so an attacker can take control over it. Another important risk is the Denial of Service (DoS) attack where the attacker takes the critical systems such as main gates and power system out of service. To resolve these risks, Cyberbit has constructed a smart solution which implements

various types of sensors for behaviorally analyzing the received data and to further detect the root cause of an attack. In Kosba, Miller, Shi, Wen, and Papamanthou (2016), authors address the lack of privacy in the existing model of the blockchain, which provides the trust on correctness of the data and availability between the two parties without the need for a third party. However, it exposes the data within blockchain which doesn't preserve privacy. They constructed a framework called Hawk for building a smart contract to preserve privacy. In their approach they formalize the blockchain model of cryptography which uses decentralized smart contract system. The system does not store clear data of transactions on the blockchain to preserve the privacy.

Blockchain has been integrated with IoT networks for enhancing the security and privacy in healthcare applications, a novel platform of IoT-based blockchain has been introduced for remote monitoring of patient vital signs using smart contracts (Jamil, Ahmad, Iqbal, & Kim, 2020). Another example of IoT-Based Blockchain integration for healthcare application is introduced in Satamraju and Malarkodi (2020), the introduced three layers framework is concerned mainly with proofing the scalability concept in healthcare.

A tele medical framework has been introduced for laboratory services in clinics and hospitals to automate the process of laboratory tests and results through IoT medical devices, and results are sent through hospital cloud services to doctors for validation and/or consultation, the proposed framework can reduce the risk of COVID-19 spreading (Celesti et al., 2020). A blockchain framework of Smart Contract System (SCS) for healthcare industry.

Another approach for protecting data privacy on blockchain is presented in Kianmajd (2017), which introduces a cryptographic layer applied over blockchain to mitigate privacy, ensuring trust and privacy are maintained. They also constructed a blockchain-based system in smart communities to share solar energy with neighbors autonomously. It also introduces a cryptographic approach to provide an access control layer over blockchain-based systems.

2.2. The use of bloackchain in healthcare systems

Blockchain technology can be used to share medical data between service providers. Authors in Xia et al. (2017) proposed a system called MedShare, which protects the privacy of data while providing an access layer over the blockchain-based model. They illustrated the problem of sharing patients' medical information with different parties. MedShare maintains a smart contract to provide access control to track and monitor any changes, or access to data in a trusted manner and with minimal risk.

In Amazon (2020) and Ghali et al. (2019), the authors provide a comprehensive introduction about modern life and the rise of big data as technology evolves in our lives. However, the authors did not explain clearly why we cannot accept the cloud-based network for sharing the medical data, as those cloud-based solutions claimed to use the most secure cryptographic algorithms. A comprehensive review of blockchain technologies in healthcare applications is introduced in Khezr, Moniruzzaman, Yassine, and Benlamri (2019), this research provides a technical study in the applications of blockchain in healthcare industries, focusing on the achievements and latest developments. Another example of four layers blockchain model for healthcare applications; the data sources, blockchain technology, healthcare applications, and stakeholders (Khezr et al., 2019).

2.3. Cloud healthcare systems

Deshmukh (2017) propose a cloud-based digital system for electronic health record in India to be scalable and able to manage data efficiently even in densely populated countries. The structure is designed to interact with the cloud server when required and to have another local medical server located at each city's health center. The system gives the patient the ability to review who accessed the medical data in compliance with current regulations such as Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). The analysis of the design eliminated the blockchain technology from the discussion although it can have the potential resolution to establish trust between the local server and the cloud server. The current structure does not ensure the integrity of the data between both servers. A novel IoT-based blockchain framework has been introduced in Dwivedi et al. (2019) to add privacy and security to the distributed network architecture in healthcare applications.

2.4. Scalabilty of the system

The normal approach of blockchain-based systems has a distributed copy of the data, contains health records and images, which requires data storage implications and a certain data throughput level of service. So, every node joining this Peer-to-Peer (P2P) network would have a copy of every health record for every citizen in the country and this would not be practical from a data storage perspective (Khezr et al., 2019). Because health data is

dynamic and expansive, replicating all health records for every member in the network would be costly, consuming network resources, and posing data throughput concerns. The blockchain functions as an access-control manager for health records and data. The actual data will reside off the blockchain itself. All data stored would be encrypted and digitally signed to ensure proper access to them (Linn & Koo, 2016). Turkanović, Hölbl, Košič, Heričko, and Kamišalić (2018) introduce a blockchain-based platform called EduCTX for a global higher education credit which can be used by different stakeholders such as students, companies, and higher education institutes. This platform works as a global unified viewpoint for verifying and checking students' education and grading records.

2.5. Risks and challenges of Blockchain-Based systems

The decentralized model of the blockchain is provided by distributing the data among the joining parties. Any joining node will get a copy of the blockchain log. This affects the speed at which the new party gets the trusted data and demands lots of storage requirements apart from the blockchain itself. Another problem is the speed of writing new data to the blockchain. The transaction processing rate will be limited to the blockchain's propagation across the network which may take several minutes to be accepted in the ledger (Bonneau et al., 2015).

2.6. The privacy and smart devices

BYOD or 'Bring Your Own Device' is a new movement in hospitals wherein medical professionals can access information on their 'own device'. This is convenient for the staff, but the lack of security associated with these devices is almost insurmountable. It is recommended that healthcare organizations create a register of all connected devices to be able to detect all unauthorized devices that could suggest security concerns (Morrow, 2012).

3. The blockchain ecosystem

This section defines the blockchain and discusses its fundamentals and major technologies; discusses the main components of blockchain as well as the processes behind it. Furthermore, it discusses the security of the blockchain and known attacks on major technologies using this model. Blockchain is a decentralized set of connected systems which run the same consensus protocol to agree upon the global state of stored data. The connected systems are referred to as nodes, and the global state is the global ledger that stores the data. The blockchain can also execute codes stored on smart contracts which are part of the ledger. In Nakamoto (2008), authors describe how blockchain has started as a record keeping system to record the transfer of digital tokens or coin such as Bitcoin and other cryptocurrencies. The ideas outlined in this whitepaper led to the world's first and largest blockchain, Bitcoin.

The Blockchain technologies provide a secure way for devices to execute any transactions using a digital immutable ledger that is distributed. The Blockchain is known as trust lessness, as long as nodes do not need to trust other nodes to interact, but they need to trust that the copy of the ledger is legitimate by validating the data using the agreed protocols. It is common that many blockchain platforms like Bitcoin or other cryptocurrencies require anonymity, while in other use cases in healthcare and other consortiums, the identity used to define and enforce permissions and role-based access (Xia et al., 2017).

3.1. Architecture types of blockchain

There are several types of systems architecture; centralized, distributed, and cloud-based. The centralized approach typically includes a single owner or small group of owners of the solution, the data which the solution work with, and the infrastructure that delivers the solution. All layers and components of the solution are owned and managed by a central authority. In the distributed solution, centralized control, ownership of the solution and the data which makes up the solution are retained. The owner of the application owns the application as well as the data, but the infrastructure may be managed by a third-party (another cloud provider) such as Amazon Web Services (AWS), Google Cloud, Microsoft Azure, IBM, etc. In the fully distributed approach, data is shared amongst all participants and the infrastructure can be shared by the solution owners, or provided by the community. Centralized and Distributed system architecture solutions usually adopt a client/server network approach (Deshmukh, 2017).

3.2. Types of the blockchain

A blockchain might be of differing types based on the use case. The public blockchain allow for the public audience to access and add data to the ledger. Bitcoin is an example of a public blockchain network. Any participant can join the network to buy, sell, or send Bitcoin to anyone else. On the other hand, a private blockchain is managed by an organization or entity that provides it to designated participants. The private blockchain is not accessible

Table 2. The mining process of the genesis block.

Step	Block ID	Nonce	SHA-256 Hash	Validated
1	1	0	d2d78c4ffc9006576da61874ee2c1a8a7fb845026774d86cbd71af97f8d080ff	No
2	1	1	7a367c017e54dc2fd7002c8bacc71b8608f3c53641efdd1698f9db9f2445c15b	No
3	1	2	be580d4923d3b38727f90146fa1a1bf4657b903eb1c831b528f356df9b360dc6	No
4	1	3	2cd300c9a23214f1ca6dcbd1453a1449166e5ed5fc00bd08ce8d852ac20253e2	No
…	…	…	…	No
156010	1	156009	0000528f976341ad8e0162d8270ac357bf2a1c5ff546d73fe18dd9d62197f541	Yes

by the public, and the ledger is only accessible by the participating nodes. The blockchain platforms may permit or deny access to its ledger by purpose. In Bitcoin, anyone has the ability to audit the public transactions executed on the ledger (Dwivedi et al., 2019).

3.3. The process of blockchain

The block is the essential component of the blockchain. It is simply the record for storing the data just as it is done on ordinary databases, but the block can have any type of structure. The structure of the block can have multiple information: The Block ID, the hash code of the block data, the previous block hash code, and list of transactions. The first block of the ledger is called Genesis because it has no previous block and the previous hash code is null or zero. If a new block is created by a participant, then an announcement is made to other nodes about the need to verify the information of the block before adding it to the local copy of the ledger. The ledger should be identical between all participating nodes. Each node is required to maintain the same consensus protocol in order to accept or reject any new block before appending it to the local copy of the ledger (Zheng, Xie, Dai, Chen, & Wang, 2017).

Table 2 illustrates the process of creating and validating a block with the following details:

- Block ID #1
- Hashing Algorithm: SHA256
- Difficulty: Four leading zeros (16-bit)
- Block Data: 'Hasan Alaswad is writing some information on the blockchain'.

The mining process starts with aggregating the content of the fields of the block, then generate the hash of them. It then checks if the generated hash is achieving the mining protocol. In the first step, the string aggregated as follows:

$$Hash = SHA256(Step\ \#\ ||\ Block\ ID\ ||\ Nonce)$$

110Hasan Alaswad is writing some information on the blockchain. (Zheng et al., 2017)

If the generated hash does not achieve the four leading zeros, then the nonce is incremented. This is an example of the difficulty of the mining process using proof of work executed by the mining participant to get his block validated and accepted by other nodes. The difficulty represents the number of leading zeros in the hashing code generated by a miner and used to regulate how long it takes for miners to add new blocks of transactions to the blockchain.

If the miner is able to solve the block validation quicker than the expected time to get winning nonce, then it is time to adjust the difficulty of the mining process. However, this is used by Bitcoin and other cryptocurrencies while the longer time requires additional computing and energy consumption, which is not suitable for other cases like in healthcare, the mining process should be expected yet safe. When the block is validated, and the hash of its content created, then it is announced to the other participating nodes in the network. Therefore, the hash of each block will always be unique based on the content of the block and any attempt to change any information of the block will result in a different hash, which requires it to be validated with the previous hash and also verified and accepted by other nodes before it is added to the chain. This gives Blockchain its property of immutability. The consensus is a way to ensure the nodes on the network verify the transactions and agree with their order and existence on the ledger. In the case of applications like cryptocurrency, this process is critical in preventing double spending or other invalid data being written to the underlying ledger, which is a database of all the transactions. A blockchain gets more secure over time. If there are more blocks confirmed that means there would be a smaller chance of a different chain to be selected as the primary one. There are two types of forks, hard, and soft. In hard fork the data is not backwards compatible. This results in a new blockchain being created. A soft fork occurs when data is backwards compatible, resulting in a change that would not create a new blockchain (Zheng et al., 2017).

3.4. The blockchain versus normal database

The blockchain is a distributed database which only has the append-only operation. In normal database systems, the access, write, update, and delete operations available, commonly referred to as the CRUD, while the blockchain is limited to only access and

write operations. In a classical database, those functions are:

- CREATE: Insert or write new records to the database.
- READ: Access existing records from the database.
- UPDATE: Change the value of existing records.
- DELETE: Remove existing records from the database.

The blockchain provides no ability to update or delete records on the database which leads to the append-only and the immutable properties of blockchain. If data is recorded on the blockchain and that data later requires alteration or is no longer relevant, that change must be recorded as an additional record on the database (Turkanović et al., 2018).

3.5. Double-Spending problem

Money is a historically accepted medium of exchange, and it is widely used as payment for goods and services. Although money can be physically a special printed paper, but it holds its value by the central authority producing it. In the modern world, the Internet connected world and trading is revolutionized by eCommerce systems like Amazon. The traditional money needs also to comply with this revolution. One of the main problems in having digital money being accepted and widely used, is that digital data can be easily duplicated or tampered with. In Nakamoto (2008), authors suggest a P2P system that solves this problem without having a central authority but requires having the majority of honest nodes participating in this network, and has introduced Bitcoin as the first decentralized digital currency, and later many other cryptocurrencies launched.

4. Security of blockchain

Li, Jiang, Chen, Luo, and Wen (2017) studied security risks and weaknesses of blockchain different technologies. They discussed a total of 17 risks in the blockchain with 12 of them in the smart contracts.

4.1. 51% attack

Li et al. (2017) studied security risks and weaknesses of different blockchain technologies. They discussed a total of 17 risks in the blockchain with 12 of them in the smart contracts. The 51% attack exploits the fact that if the consensus protocol used is the Proof of Work (PoW) and a single node has at least 51% hashing power than other participating nodes, then this node can launch a successful attack by issuing longer chain which will be accepted by remaining nodes as the truth. On the other hand, in PoS consensus protocol based blockchains, if a single node owns at least 51% of the total number of coins of the total blockchain then this node can launch a successful attack. In Piasecki (2012), authors simulated a successful attack on Bitcoin platform by creating a virtual network deployed in Google cloud service, and proved that if the malicious node has the longest chain that validates the protocol, then other nodes will accept the malicious blockchain data as the truth or trusted chain.

4.2. Private key security

In blockchain, the identity of the users is based on the public key cryptography where the private key provides the non-repudiation and considered critical to the security of the whole process, so the protection of the private keys is a must. In Bitcoin, to create a wallet you need to provide the private key using the Elliptic Curve Digital Signature Algorithm (ECDSA) cryptographic algorithm. Mayer (2016), discovered a vulnerability in the ECDSA algorithm during the signature process which allows an attacker to obtain the private key because ECDSA algorithm does not generate enough randomness. The private key cannot be recovered or regenerated by a central authority as Bitcoin is decentralized. If the private key is lost or stolen, the bitcoin account faces risks of being stolen or tampered with by attackers without consents of the owner.

4.3. Limitations of blockchain

Depending on the mining process, the blockchain can be considered inefficient consuming lots of energy like in case of Bitcoin where the mining process uses the proof-of-work. The blockchain is still a new technology and there are different technologies and implementations at its core. IBM, Microsoft, Ethereum, and Amazon all have different implementation of the blockchain model. The transaction cost and speed of public blockchains are high while the scalability is limited. The blockchain is still actively changing and evolving. Blockchain prioritizes security over speed. Therefore, solutions that require high transaction speeds are not considered good candidates for Blockchain. Most major public blockchain technologies are able to process 10–20 transactions per second worldwide. The decentralized model of the blockchain is provided by distributing the data among the joining parties, thus any node joining the network will get a copy of the blockchain log. This will affect the speed of getting the trusted data on the new party and also requires storing lots of data of the blockchain itself. Another problem is the speed of writing new data to the blockchain. The transaction processing rate will be limited to the

blockchain propagation across the network which may take several minutes to be accepted in the ledger (Bonneau et al., 2015).

4.4. Blockchain is a trend technology to 2020

The potential of blockchain technology is undeniable if implemented appropriately, it supports new business and trust models. To leverage blockchain for digital innovation, professionals must have a holistic view of the blockchain ecosystem in the region. According to Forrester research (Bennett, Cser, Hoppermann, & Da, 2017), the distributed trust systems challenge of centralized authorities is one of the ten trends that characterize how technology is transforming business as stated on their research report for top technology trends to watch in 2020. Forrester predicted that only 30% of proofs of concept will create a true foundation for blockchain in 2018. Blockchain promises to fully enable bold platform and ecosystem strategies while defending against increasing cybersecurity threats. The current projects focus on understanding the blockchain technology and how a blockchain-based working system could be beneficial in realistic systems like the smart card personal information and in I-SEHA healthcare information. In Bahrain, we are still in the phase of research and development and to be able to benefit from these researches, we need a long-term digital transformation in the territory by establishing a new trust model between the public sector and private sector organizations (The National Health Regulatory Authority (NHRA), 2020), and the open data initiative is a step in this direction.

Gartner research firm identified different systems where blockchain can be useful such as government, healthcare, manufacturing, media distribution, identity verification, title registry, and supply chain. The applications seem endless with the most obvious ones in financial applications. Blockchain can solve problems in, Healthcare Digital System, Healthcare Supply Chain Management, and IAM Security for Internet of Healthcare Things (IoHT).

4.5. Summary

In summary, several healthcare models used either PoW or Proof of Stake (POS) for consensus protocol. Nowadays, the most popular consensus mechanism used in blockchain is PoW. However, a major disadvantage of PoW is the inefficient use of computing resources and energy consumption. The current blockchain model available suffers from security issues related to the blockchain type and technologies operated. These risks are related to the consensus algorithm, the blockchain implementation, and identity management. In Sect. IV, we introduce a new concept that aims to reduce the potential security risks by the design of the blockchain topology, identity management procedures, and consensus protocols used.

5. BZKP system architecture and modeling

The proposed medical data sharing model is a blockchain-based, and the blockchain smart contracts used to create a healthcare management system can be accessed across providers. The system authenticates any user before access to provide the auditability and data sharing permissions. The main goal is to build a secure and efficient model to provide the patient data among different organizations with preserving the integrity and privacy of the patient data. The conceptual model consists of a consortium Blockchain network between the main hospitals in the Kingdom of Bahrain, a smart contracts, Web Interface and Application Programming Interface (API) for access controls the remaining organizations. The Web Interface and API offer a cost efficient solution for private hospitals which are able to access the data from any of available nodes. In the following subsection, we are going to discuss the BZKP 4-layer architecture, the BZKP blockchain model components, and the I-SEHA Digital Health System in Kingdom of Bahrain.

5.1. BZKP 4-layers architecture

The blockchain can be described as a general-purpose database, it can hold any type of data while maintaining trust and availability. In the healthcare model, the patient records will construct the basic data structure, called Health Tokens. The actual data will be stored off the blockchain itself, but its hash will be stored on the blockchain. The healthcare system processes, manages and controls the Health Tokens as medical records for the patients. These Health Tokens are stored on globally distributed P2P network where the peers of the blockchain network are the health service providers and the users of the system which can be the patients, hospitals, and connected devices. Each patient will hold a dedicated blockchain wallet. The wallet is used for collecting Health Tokens which holds the medical records and data. Anytime a new medical record is to be assigned to a patient's profile, like a new laboratory report, a new Health Token is transferred to his blockchain wallet. Blockchain technology can be used to share medical data between service providers. The proposed model is following the four-layer architecture used in Xia et al. (2017) for trustless data sharing as shown in Figure 1.

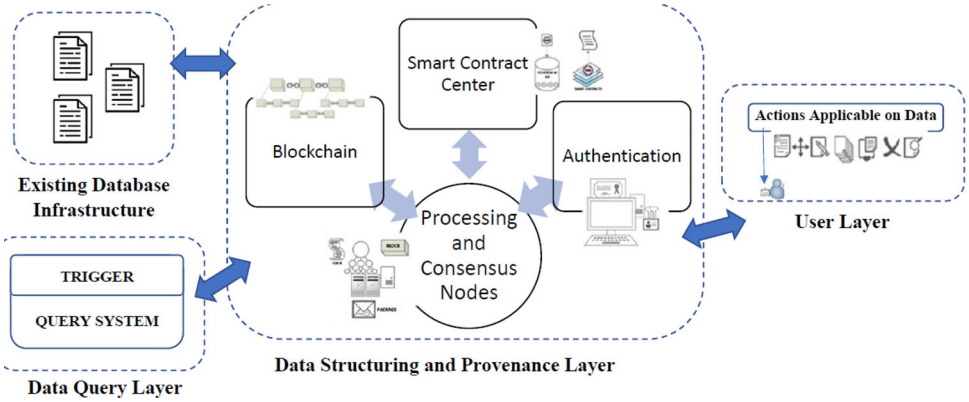

Figure 1. Four layers architecture of BZKP.

In the Kingdom of Bahrain, there are three primary health services provided for the citizens and residents: primary, secondary, and tertiary healthcare. The patient can either visit the public healthcare or the private health center. However, the current methodology of sharing data between these different organizations is based on printed reports e.g. laboratory analysis, x-ray images, and another patient's information. The main medical health records are stored in the health center in the patient permanent residency zone. The CPR card is a smart card issued to resident (Citizens and Expats) in the Kingdom of Bahrain and it contains his personal information. Each card has a unique CPR (Citizen Personal Number) number along with full name, nationality, residence address, card issue and expiry dates, blood type, and visa details for expats.

5.2. BZKP blockchain model components

The Blockchain model consists of the following main components, shown in Figure 2:

- Blockchain server is a full blockchain node with the infrastructure and the functionality of blockchain.
- A decentralized application (Dapp) which acts as an interface for the end users and other stakeholders which requires only accessing the data securely without investing in setup of the infrastructure.
- Application Programming Interface (API) is a way to interact with the blockchain server to execute a set of functions and services.
- Cloud Data Lake that provides the off-chain access of the data to be accessed by authorized clients and fully controlled.

The Blockchain's use of Public-Key Infrastructure (PKI) provides a centralized identification method using an individual's eKey public key which can be used to link that patient's record across institutions.

5.3. I-SEHA digital health system in kingdom of Bahrain

The population of the Kingdom of Bahrain is estimated to be 1.7 million (P. D. United Nations, 2017). Healthcare is provided for the residents of the kingdom regardless of their nationality, however, the Labour Market Regulatory Authority (LMRA) regulations are applied to workers in order to obtain a medical examination, conduct laboratory analyses and x-rays, and pre and postnatal care. The Supreme Council for Health in Bahrain is considered the top authority responsible for the healthcare sector. They proposed a new system to implement the Social Health Insurance Law, the new law was effective in 2019, establishing interactions between different stakeholders in regulating and monitoring healthcare sector in Bahrain. The Ministry of Health is in indirect relation with the National Health Regulatory Authority (NHRA), Hikma Pharmaceuticals, and Public environmental and social health agencies. The two main stakeholders that require access to the medical data are the services providers and buyers, as shown in Figurei 3. The main health service providers in Bahrain are Salmaniya Medical Center SMC (the main hospital in the kingdom), Bahrain Defence Force Royal Medical Services (BDF), King Hamad University Hospital, and the Public Health Centers located at different cities and towns to serve certain people based on their address of province. The regulations are applied to basic healthcare for workers including Medical examination, conducting laboratory analyses and x-rays, mother and child care including pre and postnatal, and simple dental treatment. The employer has to either sign a contract with health insurance companies licensed in the Kingdom of Bahrain or set up an integrated medical unit at the establishment and it must be licensed by the NHRA.

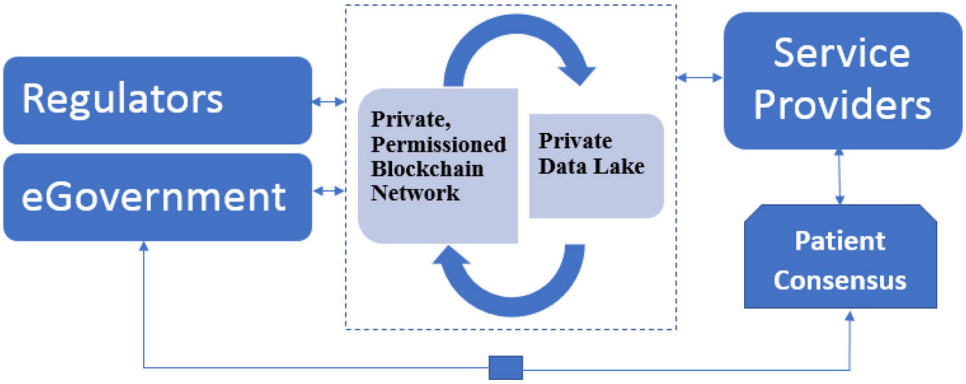

Figure 2. The blockchain model components.

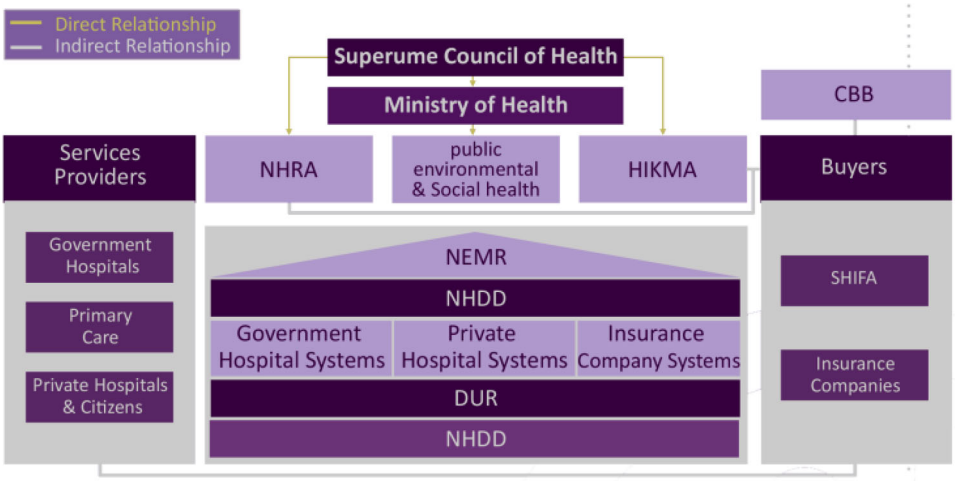

Figure 3. The proposed system for implementing SEHATI program.

The National Health Insurance Law will cover basic healthcare to provide the same health privileges for both Bahraini and expat workers registered in Bahrain. Additional medical costs other than the primary healthcare services and emergencies will be covered by the employer's health insurance provider. The employer has to pay the Ministry of Health for all workers (local or expats) in accordance with the LMRA for expats and the General Organization for Social Insurance in respect of Bahraini workers (M. of Health, 2014). According to the current law, Bahrainis will get the healthcare services for free at government facilities, while they need to pay partial amounts if they prefer private hospitals or other clinics licensed by the government. Those choosing private hospitals or clinics will have to pay no more than 40 per cent of the cost, with the government picking up the balance. The drugs and prescriptions can be dispensed from any licensed pharmacy in the Kingdom of Bahrain according to the balance for each insured patient. Table 3 shows statistics from the eServices provided by the MoH in the Kingdom of Bahrain for the period from 2015 to 2018:

The MoH has launched an electronic service and its mobile application was released in 2017, details are shown in Figure 4. The services are provided to all residents with Central Population Registry (CPR) card. The service provides the user with the ability to book an appointment with the public health centers. The user can check the blood donation information such as the last donation date and the blood type, as well as providing the radiology results by public health centers of last 30 days if available. For the user to access the current system, the user is required to log in using his CPR number, CPR Expiry Date, and Block Number.

A web version of the electronic services is also available to access some of the electronic health records. There are three basic services; Online Appointments, Patient Information, and Medical

Table 3. Statistics of the e-Services provided by the MOH in Bahrain.

eService	2015	2016	2017	2018
Patient information	0	0	48,929	57,326
Health centers and hospitals appointments	0	0	79,089	142,566
Medical certificate verification	0	0	20,376	21,821
Online registration to select family physician	0	0	0	69,115
Ask a doctor	10,452	19,301	24,635	46,159
Check blood type	84,579	19,137	23,936	39,968
Check readiness of radiology results	7,257	9,635	12,859	29,995
Limited private practice appointments	18,192	26,201	27,885	34,927
Pre-employment appointments	24263	19377	31185	39972
Death certificate services	0	0	18	1,185
Healthcare institutions	43,437	38,911	57,617	148,857

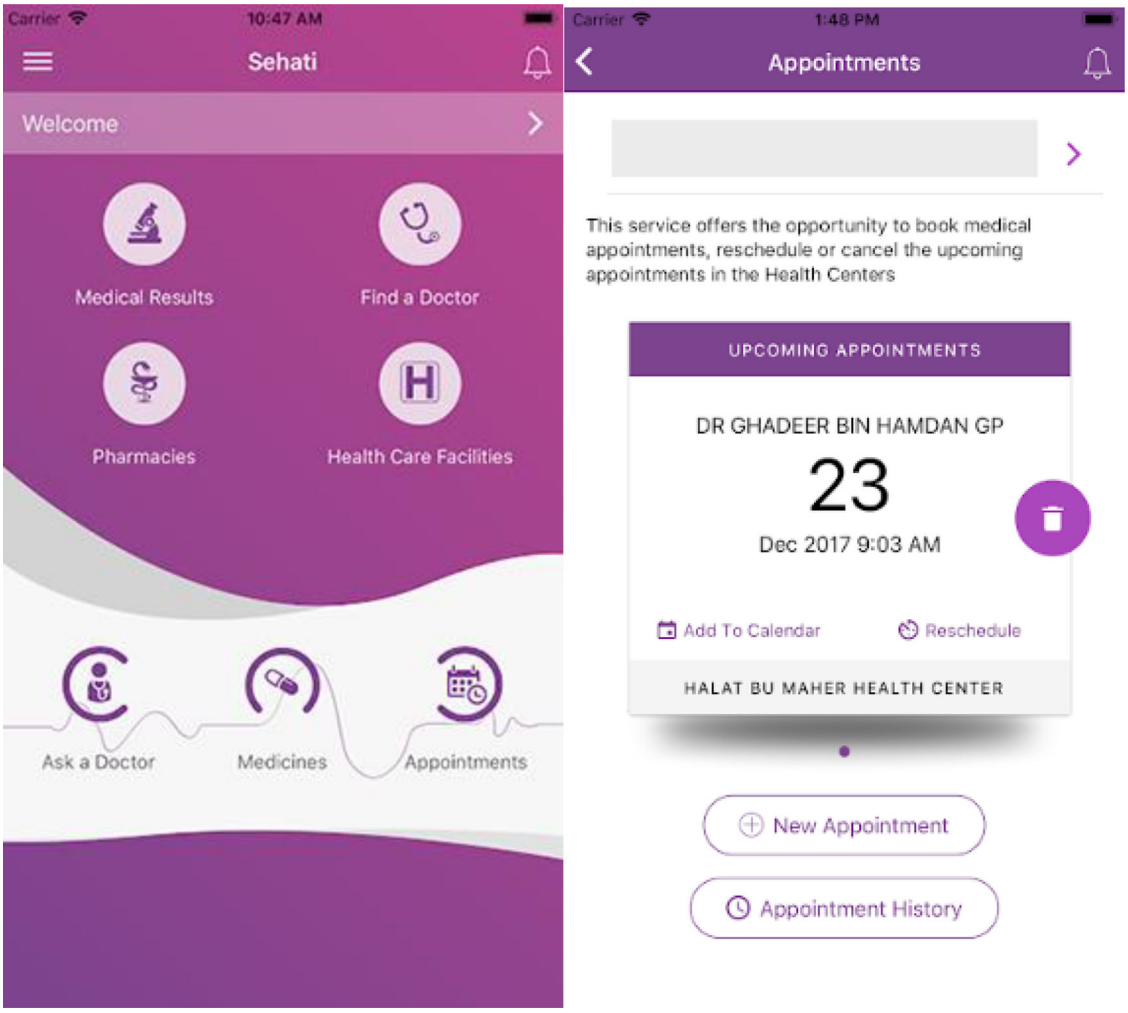

Figure 4. A mobile app (Sehati) for providing some health facilities, released by MoH.

Certificate Verification. Currently, I-SEHA has many digital services, including (M. of Health, 2019):

- Patient Information
- Online Appointments in Health Centers
- Medical Certificate Verification
- Birth Certificate
- Immunizations
- Check Readiness of Radiology Results Booking

The statistics provided by the MoH in the Kingdom show a steady use of general services like healthcare institutions contact information and checking the blood type.

However, the need for personalized services is gaining increased demands like the 'ask a doctor service', but it lacks personality as the questions are publicly visible and the patient's healthcare information is not provided with each case. Although the structure is designed to be high performance and highly scalable, the performance tests conducted show exponential increase in the response time with the increase of number of records. The performance must be asymptotically high even if the system is having millions of records.

6. Results and discussion

6.1. Risk analysis of cloud-based health information systems

In the Kingdom of Bahrain, the public and private healthcare facilities have an independent Healthcare Information Systems, while the public healthcare centers depend on I-SEHA project which is hosted centrally on MoH. In attempt to unify the data and gather all information in a single data warehouse, that is accessible by healthcare staff in all institutes, the MoH designed a system called the National Health Data Dictionary (NHDD). However, a risk of availability and DoS has been reported several times in the news since I-SEHA was launched in 2012. In August 2016, Alayam Newspaper reported a system crashes and the public health centers cannot access the system for five days and management advised to switch to manual data entry and depend on the physical files available only on the citizen designated center (Ilhamy, 2016), the system continues to face problems. In March 2019 (Unnikrishnan, 2019), the system has crashed and was out-of-service for at least two days as a result of ransomware attack. The

Table 4. Physical on-premises server requirements for one hospital.

Server Type	# Server (s)	# Core (s)	Memory (GB)
Database	1	4	64
Server	1	4	64

Table 5. 3 years total cost of ownership.

	On-Premises	AWS
Server	$ 1,177,840	$ 590,831
Storage	$ 105,347	$ 4,653
Network	$ 65,966	$ 37,525
IT-Labour	$ 3,645	$ 9,191
Total	**$ 1,352,798**	**$ 642,200**

main public hospital (BDF_Hospital, 2019) announced on twitter, for two consecutive days, that the appointments for all patients were to be postponed and switched to manual procedures in accessing patient's data by referring to the physical files.

6.2. Cost comparison between legacy and the proposed system

In addition to the security aspects discussed in the previous section between the EHR and the blockchain model, another important aspect is the cost estimation and which system cost less and perform better. Since the blockchain model proof of concept has been built using the AWS services, AWS calculator has been used in Amazon Web Services (2019) to estimate the costs of building the blockchain network of the main nodes of our case.

The estimation is based on the fact that currently individual healthcare organizations in the Kingdom of Bahrain have their local system despite that they have linked to the I-SEHA system. Although there are 6 government hospitals, 28 public health centers, and 18 private hospitals by 2015 in the Kingdom of Bahrain, the estimation will be calculated for two hospitals with minimum server requirements as shown in Table 4

The AWS estimated a total of 53% cost reduction a year by moving the physical infrastructure to AWS and utilizing a cloud infrastructure as a service. In addition, a network attached storage (NAS) with 2 TB to host the files is bought. The three-year total savings would be $710,597 as shown in Table 5.

6.3. Network-level architecture

The architecture of the model consists of two parts, data and servers. The servers provide the consortium Blockchain network of main hospitals in the Kingdom of Bahrain, and these nodes are hosted on AWS. The AWS is selected as a cloud service provider for the Blockchain with centralized ownership where the government of the Kingdom of Bahrain is the trusted authority that owns and manages the ledger and is shared with any number of parties represented by hospitals. In this way, any participating hospital has its own copy of the ledger, but the authority manages which party is invited to be part of the consortium Blockchain network. The files are stored and protected in independent instance and connected to the consortium Blockchain network using a Virtual Private Network (VPN). Any file stored in the server can also have its MD5 hash calculated for referencing using the Access Application Programming Interface (API). No file can be directly accessed except using the API to ensure the request is authorized and logged into the logging ledger.

The organizations use hybrid consensus using the Access Token and Practical byzantine fault tolerance (PBFT) consensus mechanism that gives one vote for each organization and is widely used in private Blockchain networks.

6.4. Application stack

The application stack consists of six levels, the presentation layer is the interface which can be used by the organization and patients, while it's connected to the blockchain by two levels of middleware and APIs. First using react which is a JavaScript library for building webpage user interfaces, and then the blockchain API to connect to blockchain nodes and infrastructure. The conceptual of the stack is shown in Figure 5.

6.5. The proof of beneficiary consensus algorithm

The PoW and PoS may have potential risks and require more energy consumption that affect the performance of the system. In our model, we introduced a governed consensus mechanism where the government and patient have shared authority. In this blockchain model, we introduce the concept of Process of Beneficiary as a new consensus algorithm. The process of allowing any patient to access the network by accomplishing the following two steps:

Enable Electronic Key (eKey): The government has a central authority (Information & eGovernment A (IGA), 2019) to issue electronic key (eKey) for any resident in the Kingdom of Bahrain which allows the resident to access the eGovernment services. There are two levels of the eKey, the basic and advanced. The basic level requires only registration on the website while the advanced require a fingerprint verification at the government center. The patient is required to activate the advanced level of the eKey in order to access the blockchain-based system.

Issue the Private Key: Any patient activates the advanced level of the eKey is allowed to issue the

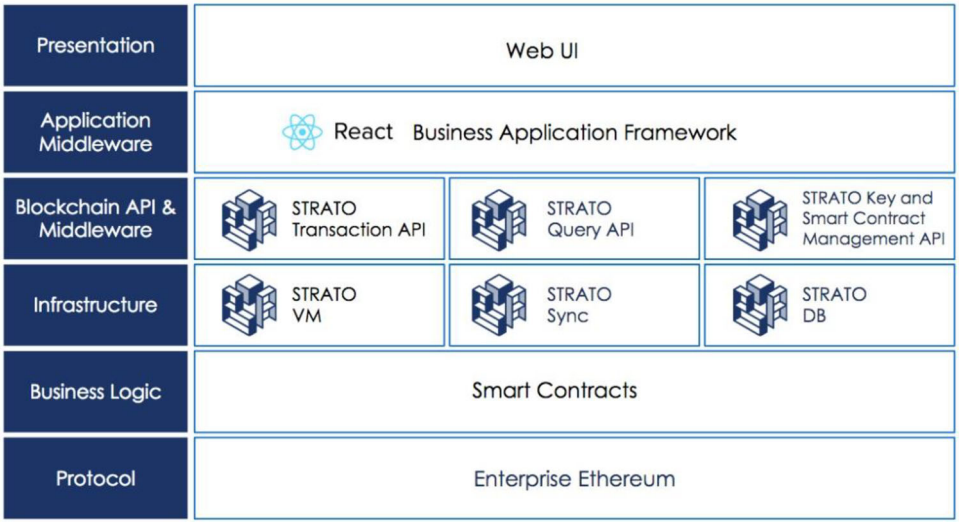

Figure 5. Application Stack conceptual model.

private key which is stored safely on his smart card. The issuance of the private key must be by visiting any government center for smart card services to ensure there is a central authority governs the process, and the patient enters his own passphrase which encrypts his private key.

The benefits of this approach are that the patient has the private key stored safely in his smart card, CPR, and can visit any government center to re-create the private key by entering a new passphrase as the private key is not recoverable. The authority uses its private key from its side to store the data and access the smart card, the two steps are illustrated in Figure 6. For a patient to access the system in a public or private center, he is requested to present his smart card and give the proper permission based on the context of the use, using the decentralized app (DApps). In addition, the patient has a mobile application and a web version which provide full details of his relevant data such as the access of his profile, or files.

6.6. Case study: LMRA expats insurance validation system enhancement

Any expat with a valid working visa in the Kingdom of Bahrain should have an active profile on LMRA, and the employer is required to pay a monthly fee to provide healthcare services to his employees. When the employee needs a healthcare service in the public sector, the health center personnel needs to refer to a system connecting the hospital with the LMRA to ensure that the patient has paid the monthly fee and thus can receive the service.

The current connection between the two independent organizations is based on a cloud system that is centrally managed by the LMRA. Many internal reports revealed that the system is having availability and outreach issues, which disrupts the service of providing the necessary healthcare service for the workers and takes a long time to verify that the worker is eligible for the service. Using the proposed blockchain model which preserves the independence between the two organizations, the MoH

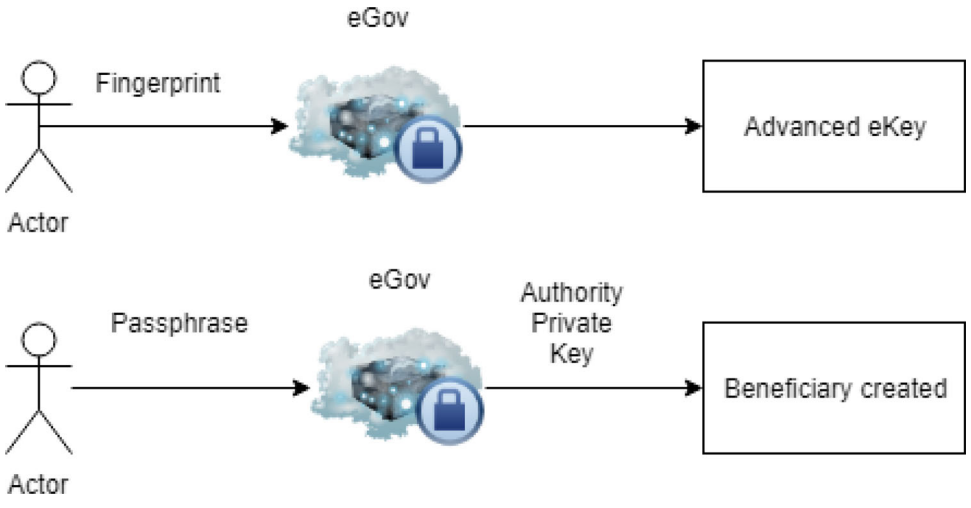

Figure 6. Creation of patient beneficiary private key.

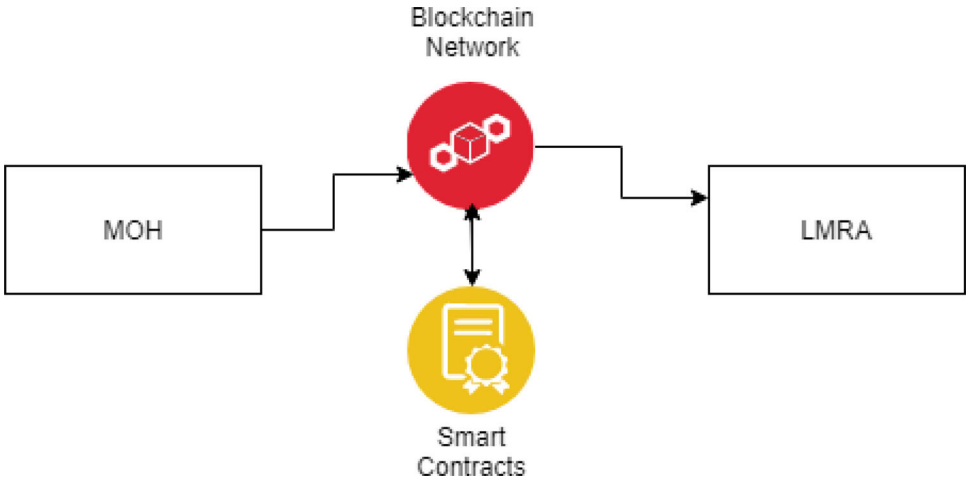

Figure 7. The interoperations between LMRA and MoH.

parties and the LMRA authority is to utilize the blockchain-based model where both are full participating nodes. The MoH will have its copy of the ledger, and the LMRA have full control and consensus over the data. In this approach which is illustrated in Figure 7, the MoH is able to enquire the blockchain for obtaining verifications of the patient visa and payment, and the smart contracts will provide the LMRA assurance that all costs are being reported and paid.

6.7. Zero-knowledge proof for prescription dispensation

The blockchain has the potential to play the main role in the digital transformation of the current process of healthcare from the central authority into full data integration to achieve end-to-end connectivity and operation as per what knows as Industry 4.0.

Al-Aswad et al. (2019) illustrate a non-interactive ZKP to prove the age of the person without revealing the exact age to the verifier using a trusted entity accessed by both parties. Using the ZKP, the private pharmacy is able to verify the medication report without affecting the privacy or integrity. The flowchart of the process of dispensing the medication can be illustrated as shown in Figure 8.

The verification of identity and prescription by the private sector can be handled using the proposed ZKP process. The verification query will be as follows: Do the patient with CPR number x have enough balance to receive medication m with quantity q?

The blockchain decentralized system acts as trusted party, steps to prove that is shown in Figure 9.

6.8. Scalability of the system

The normal approach of blockchain-based systems is to have a distributed copy of the data which contains health records, and images which require data storage implications and data throughput limitations. So, every node joining this P2P network would have a copy of every health record for every citizen in the Kingdom of Bahrain and this would not be practical from a data storage perspective. Because health data is dynamic and expansive, replicating all the health records of every member in the network would be bandwidth intensive, wasteful on network resources and pose data throughput concerns. In the presented model, the blockchain function as an access-control manager for health records and data. The actual data will reside off the blockchain itself. All data stored would be encrypted and digitally signed to ensure proper access to them (Linn & Koo, 2016).

6.9. Challenges and open research questions in moving towards blockchain solution

The blockchain has the potential to play the main role in the digital transformation of the current process of healthcare from the central authority into full data integration to achieve end-to-end connectivity and operation as per what knows as Industry 4.0. This transformation allows healthcare services to be integrated as it aligns their Operations, Technology, and People ecosystems with their Customer Solutions ecosystem (Geissbauer, Lübben, Pillsbury, & Schrauf, 2018).

- The migration from the current digital health records system to a blockchain-based are not discussed.
- The implementation of blockchain requires further awareness and the vital role management plays in ensuring the correct use of the trusted system.
- Establishing a new platform requires full collaboration from different stakeholders in agreeing on a unified platform either by joining the network or using API access.
- The decentralized model of the blockchain is provided by distributing the data among the joining parties, thus any node joining the network will

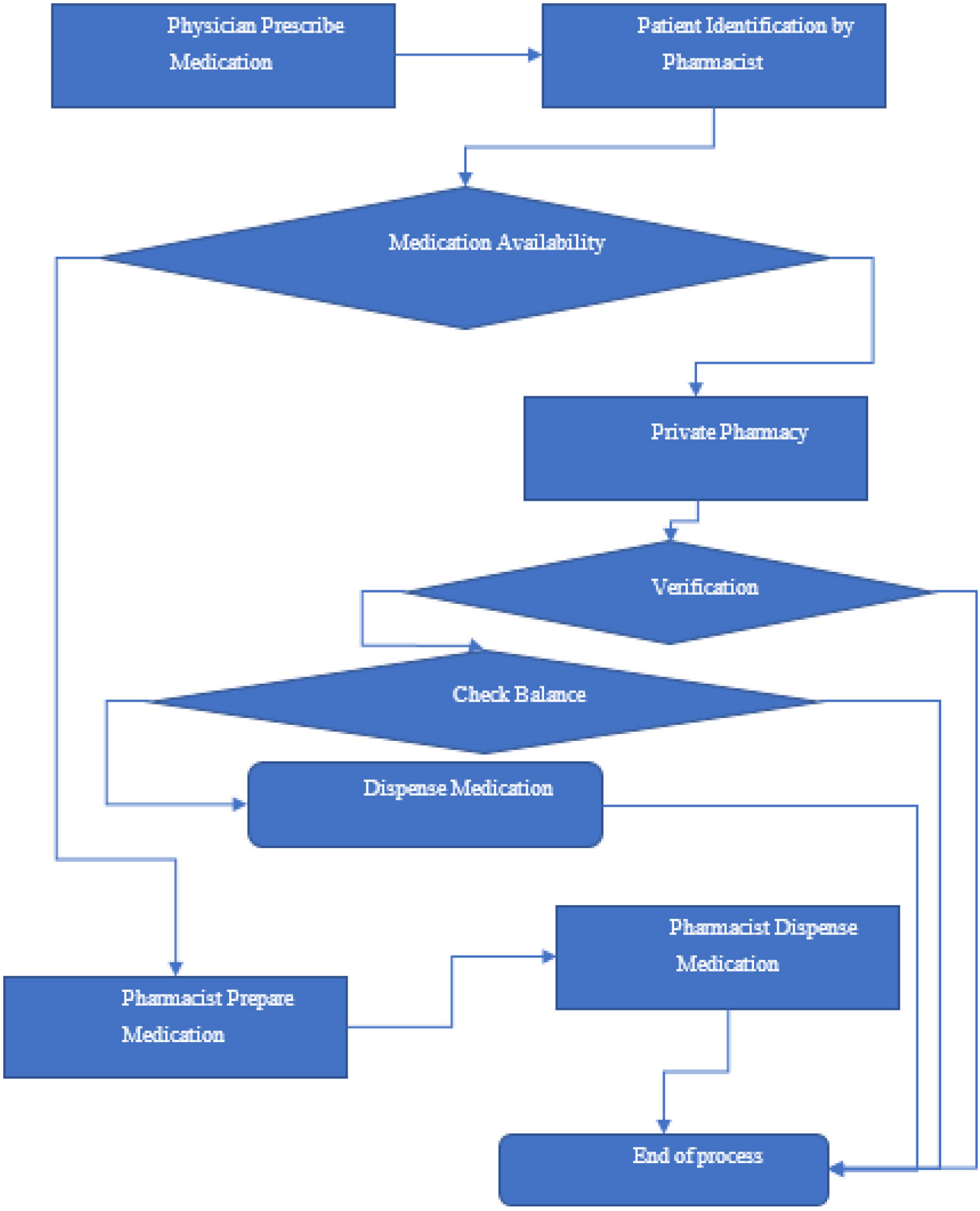

Figure 8. Medicationi dispense process flowchart.

get a copy of the blockchain log. This will affect the speed of getting the trusted data on the new party, also, this requires storing lots of data from the blockchain itself.

- The speed of writing new data to the blockchain and the transaction processing rate will be limited to the blockchain propagation across the network which may take several minutes to be accepted in the ledger (Bonneau et al., 2015).

7. Conclusion and recommendations

In this era, citizens depend on the government and private sector for getting healthcare services, the use of smart and connected devices requires a trusted model for sharing medical data with other parties without affecting the privacy or integrity of the data. In this paper, we proposed a blockchain-based model that addresses the interoperability among

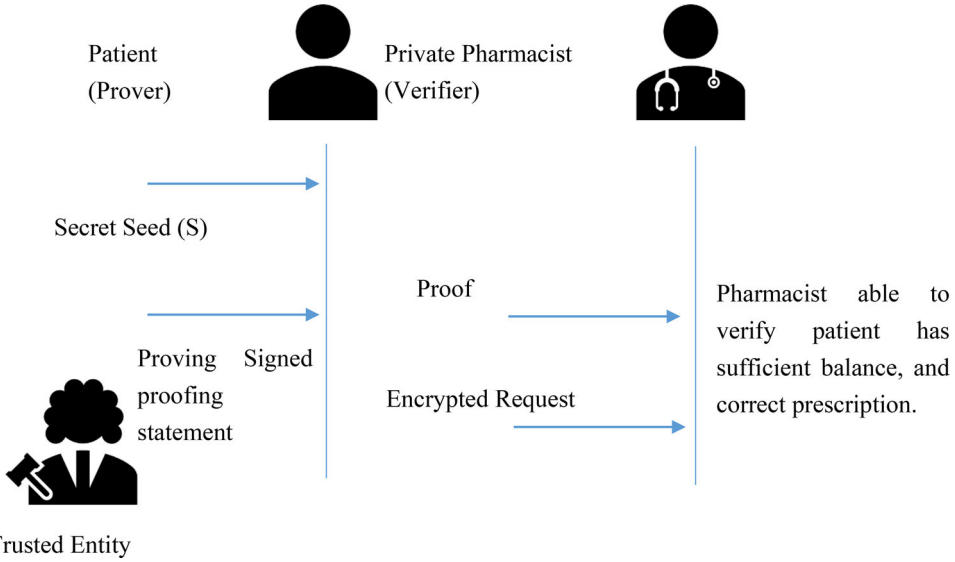

Figure 9. Zero-knowledge proof process for medication dispense in the private sector.

different stakeholders in the Kingdom of Bahrain by providing trusted communication of data to share medical data among them while protecting the integrity of the data by providing a reliable method for accessing data without affecting confidentiality, and to providing a strong and trusted audit log of which data was accessed by whom. Using the blockchain enhances the availability of the healthcare data. If the network connection is lost to the Internet, then the node is still able to refer to its local trusted data and it is not required to repeat the same test multiple times which cost more and waste time.

According to international experiments and urban development, the development of networking connectivity such as 5G will enable real-time connectivity between different IoT devices and can connect everything. Healthcare is one of the key sectors in smart cities and it shows the importance of developing a unified trust model for sharing data between stakeholders requiring access to the shared data. Although blockchain technology offers numerous opportunities for healthcare, it is considered relatively new and further risk analysis needs to be performed to compare the blockchain-based models with cloud-based models. In addition, several technical and organizational challenges must be addressed before a healthcare blockchain-based model can be adopted by the healthcare sector in Bahrain including the migration of data from the current integrated electronic system I-SEHA As a future project, there is a need to develop a unified blockchain-based model for a trusted network across smart city hubs. Our recommendations to address the privacy and secure sharing of healthcare data are:

1. That authorities allow any person to update the smart card with his own private key for any IoT devices and private sectors interact using the blockchain system.
2. Leveraging Amazon Web Services to host the blockchain nodes to reduce the costs, and the hosted servers in the Kingdom of Bahrain will provide the best connectivity between different institutions while reducing maintenance and electricity costs. This is aligned with Bahrain's vision 2030 and UN 2030 sustainable development goals.
3. Enable the MOH to develop blood donations DApps integrated with the main patient's data for blood type and provide a database of donors and their donation activities.
4. Utilize the healthcare blockchain system for secure automated remote patient monitoring using smart contracts.
5. Integration of the zero-knowledge proof with the blockchain allowing executing queries to the blockchain without leaking additional information thus protecting the privacy of the patient data.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Al-Aswad, H., Hasan, H., Elmedany, W., Ali, M., & Balakrishna, C. (2019). *Towards a blockchain-based zero-knowledge model for secure data sharing and access*. 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 76–81. doi:10.1109/FiCloudW.2019.00027

Alharam, A. K., & El-Madany, W. (2017a). Complexity of cyber security architecture for IoT healthcare industry: A comparative study. 2017 5th International Conference

on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 246–250.

Alharam, A. K., & El-Madany, W. (2017b). *The effects of cyber-security on healthcare industry*. 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), pp. 1–9. doi:10.1109/IEEEGCC.2017.8448206

Alromaihi, S., Elmedany, W., & Balakrishna, C. (2018). Cyber security challenges of deploying IoT in smart cities for healthcare applications. 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 140–145. doi:10.1109/W-FiCloud.2018.00028

Amazon Web Services. (2019). AWS total cost of ownership (TCO) calculator. Retrieved July 31, 2020, from https://aws.amazon.com/tco-calculator/

Amazon. (2020). AWS Cloud Security. Retrieved July 31, 2020, from https://aws.amazon.com/security/

BDF_Hospital. (2019). BDF hospital disclaimer and apology. Retrieved July 31, 2020, from https://www.bdfmedical.org/disclaimer/

Bennett, M., Cser, A., Hoppermann, J., & Da, C. (2017). Predictions 2018: Be ready to face the realities behind the blockchain hype. Retrieved July 31, 2020, from https://www.forrester.com/report/Predictions+2018+Be+Ready+To+Face+The+Realities+Behind+The+Blockchain+Hype/-/E-RES140115

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). *Sok: Research perspectives and challenges for Bitcoin and cryptocurrencies*. 2015 IEEE Symposium on Security and Privacy (SP), pp. 104–121.

Celesti, A., Ruggeri, A., Fazio, M., Galletta, A., Villari, M., & Romano, A. (2020). Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. *Sensors*, *20*(9), 2590. doi:10.3390/s20092590

Deshmukh, P. (2017). Design of cloud security in the EHR for Indian healthcare services. *Journal of King Saud University - Computer and Information Sciences*, *29*(3), 281–287. doi:10.1016/j.jksuci.2016.01.002

Djenna, A., & Saïdouni, D. E. (2018). *Cyber attacks classification in IoT-based-healthcare infrastructure*. 2018 2nd Cyber Security in Networking Conference (CSNet), pp. 1–4. doi:10.1109/CSNET.2018.8602974

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In *AMIA annual symposium proceedings* (Vol. 2017, p. 650). American Medical Informatics Association.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, *19*(2), 326. doi:10.3390/s19020326

Geissbauer, R., Lübben, E., Pillsbury, S., & Schrauf, S. (2018). *How industry leaders build integrated operations ecosystems to deliver end-to-end customer solutions*. PwC Strateg.

Ghali, C., Stubblefield, A., Knapp, E., Li, J., Schmidt, B., & Boeuf, J. (2019). Application layer transport security. Retrieved July 31, 2020, from https://rwc.iacr.org/2019/slides/Application%20Layer%20Transport%20Security.pdf

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2019). Blockchain in healthcare and health sciences—a scoping review. *International Journal of Medical Informatics*, *134*, 104040.

Ilhamy, A. (2016). Electronic system crashes confuse doctors and reviewers. *Alayam Newspaper*. Retrieved July 31, 2020, from https://www.alayam.com/epaper

Information & eGovernment A (iGA) of Bahrain. (2016). Bahrain in figures. Retrieved July 31, 2020, from http://www.data.gov.bh/ar/ResourceCenter/DownloadFile?id=2712

Information & eGovernment A (IGA). (2019). eKey Bahrain. Retrieved July 31, 2020, from https://www.facebook.com/iGABahrain/posts/what-is-ekey-why-should-you-have-itthe-ekey-is-a-single-sign-on-authentication-s/2687899331225046/

Jamil, F., Ahmad, S., Iqbal, N., & Kim, D.-H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*, *20*(8), 2195. doi:10.3390/s20082195

Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, *55*, 102018. doi:10.1016/j.scs.2020.102018

Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. *Electronics*, *9*(1), 94. doi:10.3390/electronics9010094

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51–59. doi:10.1109/MCOM.2017.1600297CM

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences*, *9*(9), 1736. doi:10.3390/app9091736

Kianmajd, P. (2017). *Protecting data privacy in the presence of data provenance*. University of California, Davis. Retrieved July 31, 2020, from https://books.google.com.bh/books/about/Protecting_Data_Privacy_in_the_Presence.html?id=Qq3dtAEACAAJ&redir_esc=y

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*. 2016 IEEE Symposium on Security and Privacy (SP), pp. 839–858.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, pp.841-853 doi:10.1016/j.future.2017.08.020

Linn, L. A., & Koo, M. B. (2016). *Blockchain for health data and its potential use in health it and health care related research*. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland: ONC/NIST.

M. of Health. (2014). Order No. (29) of 2014 with regard to specifying and regulating basic health care for workers of corporations. Available on: https://lmra.bh/portal/en/legal/show/50. Retrieved July 31, 2020.

M. of Health. (2019). About MOH e-services. Retrieved July 31, 2020, from https://www.moh.gov.bh/eServices?lang=en#:~:text=As%20part%20of%20MOH's%20commitment,birth%20and%20death%20certificates%20services

Mayer, H. (2016). ECDSA security in bitcoin and ethereum: A research survey. *Blog.Coinfabrik*. Retrieved July 31, 2020, from https://www.semanticscholar.org/paper/ECDSA-Security-in-Bitcoin-and-Ethereum-%3A-a-Research-Mayer/434a117a2717cdbf78035365d8bab2b0a3410be9

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8. doi:10.1016/S1353-4858(12)70111-3

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Journal for General Philosophy of Science*, 39(1), 53–67. doi:10.1007/s10838-008-9062-0

P. D. United Nations. (2017). World population prospects: The 2017 revision. Department of Economic and Social Affairs. Retrieved July 31, 2020, from https://esa.un.org/unpd/wpp/Publications/Files/WPP2017_KeyFindings.pdf

Piasecki, P. (2012). Design and security analysis of Bitcoin infrastructure using application deployed on Google Apps Engine, pp. 1–89. Retrieved July 31, 2020, from https://www.mn.uio.no/ifi/studier/masteroppgaver/conserns/piaseckimscgoodreading12design-and-security-analysis-of-bitcoin-infrastructure.pdf

S. Council of Health. (2017). National Social Health Insurance Program. Retrieved July 31, 2020, from https://www.bahrain.bh/reproductivehealthcare

Satamraju, K. P., & Malarkodi, B. (2020). Proof of concept of scalable integration of internet of things and blockchain in healthcare. *Sensors*, *20*(5), 1389. doi:10.3390/s20051389

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407.

The National Health Regulatory Authority (NHRA). (2020). 2016 report. Retrieved July 31, 2020, from https://www.nhra.bh/About/AnnualReport/

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, *6*, 5112–5127. doi:10.1109/ACCESS.2018.2789929

Unnikrishnan, R. (2019). Probe after data network crashes, GDN Online. Retrieved July 31, 2020, from http://www.gdnonline.com/Details/510728/Probe-after-data-network-crashes

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, *5*, 14757–14767. doi:10.1109/ACCESS.2017.2730843

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794–2830. doi:10.1109/COMST.2019.2899617

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends*. Proceedings of the 2017 IEEE 6th International Congress on Big Data: BigData Congress, October, pp. 557–564, doi:10.1109/BigDataCongress.2017.85